UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* INFORMATION ASSOCIATED WITH JUANALVARADO9231@ICLOUD.COM THAT IS STORED AT PREMISES CONTROLLED BY APPLE INC.	)	Case No. 25-mj-682

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A, incorporated herein.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. § 841 and 18 U.S.C. § 922(g)	Distribution of controlled substances and possession of a firearm by a felon.

The application is based on these facts:

See attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____*)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

s/ Matthew W. King
Applicant's signature

Matthew W. King, Special Agent FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 3/31/2025

/s/ Jose R. Arteaga
Judge's signature

City and state: Philadelphia, PA

HONORABLE JOSE R. ARTEAGA, U.S.M.J.
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH JUANALVARADO9231@ICLOUD.COM THAT IS STORED AT PREMISES CONTROLLED BY APPLE INC.	Case No. 25-mj-682

AFFIDAVIT IN SUPPORT OF AN
APPLICATION FOR A SEARCH WARRANT

I, Special Agent Matthew W. King, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account assigned with the Apple ID juanalvarado9231@icloud.com (the "Target Apple Account") that is stored at premises owned, maintained, controlled, or operated by Apple Inc. ("Apple"), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since March 2008. During my tenure with the FBI, I have received specialized training and

experience in narcotics smuggling and distribution investigations, including but not limited to, the means and methods used by traffickers to import and distribute narcotics, interdiction, smuggling methods, and the concealment and laundering of proceeds from illicit drug trafficking activities. During my tenure as an agent, I have participated in and personally conducted several investigations involving illicit narcotics trafficking. Based on my training and experience, I know that drug traffickers utilize cellular phones to further their drug trafficking activities by coordinating meetings during which drugs and/or drug proceeds are exchanged. Prior to my employment with FBI, I was employed as a Deputy Attorney General with the Delaware Attorney General's Office.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 21 U.S.C. § 841 (distribution of controlled substances) and 18 U.S.C. § 922(g) (possession of a firearm by a felon) have been committed by JUAN ALVARADO. There is also probable cause to search the information described in Attachment A for evidence of these crimes as further described in Attachment B.

PROBABLE CAUSE

5. In late April 2022, Joseph Domico, a Task Force Officer (TFO) with the FBI, Martin Sheeron, also a TFO with the FBI, and other Special Agents from the FBI started an investigation into JUAN ALVARADO. The FBI developed sources of information who stated

that ALVARADO was suppling large quantities of fentanyl and marijuana to people in the Philadelphia area out of 4019 "O" Street and 1703-05 Worrell Street.

6. On April 29, 2022, at approximately 1:00 pm, TFO Domico, TFO Sheeron and your affiant, along with other members of law enforcement, set up surveillance at 1703-05 Worrell Street. At approximately 1:45 pm, TFO Domico and your affiant met a confidential informant[1]. The CI and his vehicle were searched for narcotics, United States Currency, and contraband with negative results. The CI was supplied with a recording device and was directed

---

[1] The CI, who is in a position to testify, is a documented source of information who has cooperated with investigators of the FBI and the Philadelphia Police Department (PPD) since April 2022. The CI was arrested by PPD in March, 2022. As a result of this arrest, the CI was charged by state authorities with felony possession with intent to distribute heroin. These charges were later dropped in return for the CI's cooperation with FBI and PPD. The CI continues to provide information to the FBI. The CI has a criminal record, involving convictions for simple possession of heroin, conspiracy to distribute narcotics, firearms, and possession with intent to distribute narcotics. The CI has not received financial compensation for his/her recent cooperation with the FBI. The CI has provided information that has been corroborated and has significantly advanced several FBI investigations. On November 15, 2022, your affiant received a call from the Drug Enforcement Administration ("DEA") in Wilmington, Delaware about an investigation they were conducting in the Philadelphia area. During the course of their investigation, the DEA made a controlled narcotics purchase from a person they believed to be the CI. The DEA source who made the buy knew the CI from doing business with the CI years ago and reported to the DEA that the CI was the person who sold the source the drugs during the controlled purchase. In addition, the vehicle used by the target of the DEA investigation was the same make and model as one that investigators have seen the CI utilize. Thus, as of November 15, 2022, the CI appeared to be conducting illegal activities. During the CI's debriefings and handling as a confidential informant, the CI was repeatedly instructed by the FBI not to engage in any criminal conduct and that doing so would result in termination of CI's cooperation. Prior to the FBI becoming aware of the CI's unapproved criminal conduct, the FBI believed, and continues to believe, that the CI's information was reliable as it was independently corroborated by other information and means of investigation and was consistent with other known evidence. The FBI continues to believe that the CI's previously provided truthful information, including that which is contained or incorporated within this affidavit is accurate and reliable.

to place a call to ALVARADO. The CI placed a call to ALVARADO at 267-423-1347 to discuss obtaining a sample of heroin/fentanyl. The CI was told to come to the shop (which the CI took to mean 1703-05 Worrell Street). At approximately 1:55 pm, the CI arrived at the shop and ALVARADO exited 1703-05 Worrell Street and walked to the CI's vehicle. ALVARADO entered the passenger seat. At approximately 2:05 pm, a then-unidentified Hispanic male exited 1703-05 Worrell Street and walked over to the passenger side window of the CI's vehicle. The male tossed a clear baggie inside. At approximately 2:09 pm, the CI overheard ALVARADO call someone named "Lex" and tell "Lex" ALVARADO needed a sample triple the size of the one the male brought out. The unidentified Hispanic male then exited the back door of 1703-05 Worrell Street walked to the passenger side of the CI's car and after a brief conversation walked to 4019 "O" Street. The Hispanic male then went to a white door at the rear of the property and went inside. At approximately 2:18 pm, the Hispanic male exited the rear white door of 4019 "O" Street got into a dark grey Mazda 3 with a Delaware paper tag, went back to 1703-05 Worrell Street, and handed a clear bag to ALVARADO through the passenger side window of the CI's vehicle. ALVARADO then exited the vehicle and went back to the Worrell Street address. The CI then returned to TFO Domico and your affiant and handed over one bag containing approximately 7 grams and one bag containing approximately 15 grams of suspected fentanyl. The lab results show that the net amount was 9 grams of fentanyl.

7. On Monday, May 2, 2022, at approximately 5:13pm, TFO Domico and your affiant met the CI again. The CI and his vehicle were searched for narcotics, United States Currency, and contraband with negative results. The CI was supplied with a recording device and directed to call ALVARADO at 267-423-1347. The CI placed that call and was directed to come to the shop (1703-05 Worrell Street). Other members of law enforcement set up surveillance at

Worrell and O Streets. At approximately 5:20 pm, the CI arrived at 1703-05 Worrell Street and ALVARADO exited the back door and got into the passenger side of the CI's vehicle. At approximately 6:50 pm, the CI and ALVARADO pulled up in front of 4019 "O" Street, ALVARADO exited the vehicle, and walked inside through a white door in the rear of the property. At approximately 6:57 pm, ALVARADO exited the property with a true religion black satchel and got back into the CI's vehicle. The vehicle was then followed back to 1703-05 Worrell Street. At approximately 7:05 pm, ALVARADO exited and got into a grey Chrysler 300 and left the area. The CI then returned to TFO Domico and your affiant and handed over the black true religion satchel containing 1 clear zip locked baggie containing 1 red and one white square object with iPhone written on it containing approximately 875 grams of bulk heroin/fentanyl. The lab later confirmed that this was 834 grams of fentanyl. This distribution was on consignment. The CI did not provide ALVARADO with any money. The set up to the sale discussed the CI paying ALVARADO once the CI sold the "kilo."

8. On Wednesday, May 4, 2022, at approximately 2:30 pm, surveillance was set up by law enforcement at 4019 "O" Street and 1703-05 Worrell Street. At approximately 2:50 pm, ALVARADO was stopped near 4500 Whitaker Avenue while driving a black tinted Hyundai Genesis PA Tag #LYD4671. TFO Domico recovered $7,465.00 from ALVARADO from his black satchel. At approximately 2:55 pm, FBI SWAT executed local search and seizure warrants for 4019 "O" Street and 1703-05 Worrell Street. Recovered from 1703-05 Worrell Street were three pages containing alleged tally sheets. From 4019 "O" Street, agents/TFOs recovered the following: from the first floor, 3 digital scales, one court paperwork and probation card in the name of Alex Rodriguez, identified by TFO Domico as the Hispanic male from the first distribution, 3 note books containing tally work, $947.00 in cash, 12 large heat-sealed bags

marked "Zealousy," 14 large heat-sealed bags marked "White Runiz," one marked "laughing Gas," 4 marked "lemon Cherry _Gelato," one marked "ZA cream cake, two marked "Waffle cone," two marked "Sweets," 3 black heat-sealed baggies all containing alleged marijuana, 14 sealed packets stamped "High Monkey," 9 sealed packets marked "spaceman," 3 packets stamped "Midnight Sprinkles," all containing marijuana, as well as one Walgreens pill bottle containing numerous M30 pills containing suspected fentanyl. Recovered from the couch was one Walther, Mod PPQ M2 Pro M Series .40 caliber semi-automatic handgun, serial #FCM6105, loaded with one magazine with 13 live rounds. Recovered from the rear bedroom dresser were one Glock model 30, .45 caliber semi-automatic handgun, serial #WFC484, loaded with one 10-round magazine with ten live rounds; one Springfield Armory Model XDs-9, serial #HG16394, with a laser, loaded with one 9-round magazine with 9 live rounds; one Glock model 22, .40 caliber semi-automatic handgun with auto sear, an obliterated serial #, loaded with one 12-round magazine with 12 live rounds; one Smith and Wesson model M&P 40 performance .40 caliber semi-automatic handgun, serial #HKD8708, with Viper Optic stream light flashlight, loaded with one 15-round magazine with 15 live rounds; one Smith and Wesson model M&P Pro Series 9mm semi-automatic handgun, serial #HRZ6372, loaded with one 17-round magazine with 17 live rounds; one extended magazine with 21 .40 caliber rounds; and one box of 35 rounds of .40 caliber ammunition. A federal consent was obtained by Officer Clarke from Juan ALVARADO for DNA. ALVARADO's DNA was on the Walther, Mod PPQ M2.

9. ALVARADO told law enforcement on the day of the search warrant that he could help them secure an additional two kilos and possibly make an arrest. Law enforcement agreed to let ALVARADO engage in this limited cooperation but advised him that he would be going to the local jail that night. ALVARADO made a call, ostensibly set up a deal, and was given a

recorder by the FBI. When it came time for the meet, however, ALVARADO tossed the recorder and fled. This is the same recorder used previously for the buys and recordings.

10. On Friday May 20, 2022, the CI contacted TFO Domico with a phone number 267-621-6377 for ALVARADO. The CI also stated that ALVARADO had purchased a new handgun and a large amount of narcotics. Location information was obtained by members of the FBI which placed the phone around the area of 7600 Roosevelt Blvd. which is the Roosevelt Inn. On Wednesday, May 25, 2022, surveillance was set up, ALVARADO exited the front of the Roosevelt Inn and got into a black Honda civic which was lost in the area. On May 26, 2022, at approximately 1:33 pm, law enforcement executed a search warrant on 7600 Roosevelt Blvd. Room #144. ALVARADO was arrested by law enforcement. Recovered from a drawer in his room was one black baggie containing clear and black baggies that contained approximately 330 grams of suspected marijuana. Also, in the drawer was approximately $41,047.

11. ALVARADO consented to the search of his iPhone, that was recovered at the time of his arrest. This was the phone with phone number 267-621-6377. A search of that phone revealed that the Apple ID associated with the device was otre215@icloud.com.

12. A review of the physical phone revealed the following:

a. The phone has an internet search history that includes, “how to know if someone wanted,” “Most Wanted – FBI,” “Federal Bureau of Investigation,” and related searches. All these searches come just hours before the defendant’s arrest.

b. There are multiple videos of the defendant himself as well as videos of money and what appears to be marijuana.

c. The phone appears to have been activated just hours after ALVARADO fled from law enforcement (May 4, 2022, at 9:02 pm).

d. It appears on May 4, 2022, the phone was activated with the otre215@icloud.com.

13. March 28, 2025, Apple provided information pursuant to a federal subpoena requesting information associated with, among other things, JUAN ALVARADO and phone number 267-423-1347. Apple responded and stated that phone number 267-423-1347 was associated with iCloud account juanalvarado9231@icloud.com.

14. As noted in more detail below, Apple offers a variety of services and features associated with iCloud accounts. This account has the following features enabled, bookmarks, calendars, iCloud photos, iCloud drive, mail, mail header, notes, and sign in with apple. November 18, 2020, was the date of activation for iCloud account juanalvarado9231@icloud.com. The account, based on the returns, was active up to and including the time of the above-described conduct. Based on my training and experience I believe that evidence of the above-described criminal conduct will be found in the iCloud account juanalvarado9231@icloud.com. The features enabled in the iCloud account include photographs, calendar information and mail which there is probable cause to believe will contain evidence of the above-described criminal conduct. This especially true given the evidence that was obtained from ALVARADO's phone obtained at the time of his arrest which contained photographs of criminal activity and searches for information relevant to this investigation.

APPLE ACCOUNTS AND APPLE ID

15. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

16. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other

documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of iOS devices, as well as share their location with other iOS users. It also allows owners of Apple devices to manage, interact with, and locate AirTags, which are tracking devices sold by Apple.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content,

including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

17. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

18. Apple captures information associated with the creation and use of an¬ Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status ¬¬of the account (including whether the account is inactive or closed), the methods used to

connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

19. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "capability query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the "Find My" service, including connection logs and requests to remotely find, lock, or erase a device, are also maintained by Apple.

20. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

21. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Some of this data is stored on Apple's servers in an encrypted form but may nonetheless be decrypted by Apple. Records and data associated with third-party apps, including the instant messaging service WhatsApp, may also be stored on iCloud.

22. The evidence developed in this investigation, as presented above, indicates that ALVARADO used phones, including Apple devices and Apple accounts, to sell illicit drugs. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

23. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a

search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

24. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement). We know in this case that ALVARADO did not have the phone used during the controlled buys on his person at the time of his arrest. This was likely because it contained incriminating evidence. There is probable cause to believe that evidence of his drug dealing is contained in his iCloud account.

25. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

26. 126. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

AUTHORIZATION REQUEST

27. Based on the foregoing, I request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

28. Based on the forgoing, I submit that there is probable cause to believe that violations of 21 U.S.C. § 841 (distribution of controlled substances) and 18 U.S.C. § 922(g) (possession of a firearm by a felon) were committed by JUAN ALVARADO and others, associated with associated with the Target Apple Account; that this Apple account was used in furtherance of these crimes; and contains evidence of those violations. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B. I therefore request the warrant be issued for the search of the Apple account.

Respectfully submitted,

s/ Matthew W. King

Matthew W. King
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to by telephone on March 31, 2025.

/s/ Jose R. Arteaga
HONORABLE JOSE R. ARTEAGA
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the below Apple accounts that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at One Apple Park Way, Cupertino, California.

a. juanalvarado9231@icloud.com

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple Inc. ("Apple")

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A::

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers

("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging

and capability query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My and AirTag logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with AirTags, Location Services, Find My, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

II. Information to be Seized by the Government

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of 21 U.S.C. § 841 (distribution of controlled substances) and 18 U.S.C. § 922(g) (possession of a firearm by a felon) (hereinafter "Subject Offenses") as described in the affidavit submitted in support of this Warrant, including, for each account, information pertaining to the following matters, from April 1 2022, to May 27, 2022:

a) Information that constitutes evidence of the identification or location of the user(s) of the target accounts;

b) Information that constitutes evidence concerning persons who (i) collaborated, conspired, or assisted (knowingly or unknowingly) in the commission of the Subject Offenses; or (ii) communicated with the target accounts about matters relating to the Subject Offenses, including records that help reveal their identities and whereabouts;

c) The identity of the person(s) who communicated with the target accounts or any associated user ID about matters relating to the laundering of funds;

d) Information that constitutes evidence indicating the target accounts user's state of mind, e.g., intent, absence of mistake, or evidence indicating preparation or planning, related to the Subject Offenses;

e) Information that constitutes evidence concerning how and when the target accounts were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the Subject Offenses and to the Account user;

f) All banking and business records;

g) Information that constitutes evidence concerning the amount and location of any U.S. dollar payments, monies, or funds transfers;

h) Information that constitutes evidence related to controlled substances, including the diversion, transportation, shipment, smuggling, storage, sale and/or distribution.

i) Information that constitutes evidence regarding the transportation or transmission of funds that have been derived from the commission of the Subject Offenses;

j) Information that constitutes evidence transportation, transmission, or transfer of funds that are intended to be used to promote, conceal, or support unlawful activity; and

k) All communications between/among the owners of the target accounts and others regarding the Subject Offenses.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by **Apple Inc.** ("Apple"), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google. The attached records consist of _____ **electronic information**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, and they were made by Google as a regular practice; and

b. such records were generated by Google's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of

the Federal Rules of Evidence.

Date	Signature

AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means Original Duplicate Original

UNITED STATES DISTRICT COURT

for the

Eastern District of Pennsylvania

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
INFORMATION ASSOCIATED WITH JUANALVARADO9231@ICLOUD.COM THAT IS STORED AT PREMISES CONTROLLED BY APPLE INC.

Case No. 25-mj-682

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Northern District of California

(identify the person or describe the property to be searched and give its location):

See Attachment A, incorporated herein.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein.

YOU ARE COMMANDED to execute this warrant on or before April 14, 2025 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to DUTY MAGISTRATE JUDGE .
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____ .

Date and time issued: 3/31/2025 at 3:32p.m.

/s/ Jose R. Arteaga
Judge's signature

City and state: Philadelphia, Pa

HONORABLE JOSE R. ARTEAGA, U.S.M.J.
Printed name and title

Return

Case No.: 25-mj-682	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____

Executing officer's signature

_____

Printed name and title